WSP ACCESS CJIS PHYSICAL PROTECTION

210.1 PURPOSE

The purpose of this policy is to provide guidance for agency personnel, support personnel, and private contractors/vendors for the physical, logical, and electronic protection of Criminal Justice Information (CJI). All physical, logical, and electronic access must be properly documented, authorized and controlled on devices that store, process, or transmit unencrypted CJI. This Physical Protection Policy focuses on the appropriate access control methods needed to protect the full lifecycle of CJI from insider and outsider threats

210.2 POLICY

All physical, logical, and electronic access must be properly documented, authorized and controlled on devices that store, process, or transmit unencrypted CJI. This Physical Protection Policy focuses on the appropriate access control methods needed to protect the full lifecycle of CJI from insider and outsider threats.

210.3 DEFINITIONS

CJI: Criminal Justice Information

CJIS: Criminal Justice Information System

Physically Secure Location: A physically secure location is a facility, a criminal justice conveyance or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect the FBI CJI and associated information systems. The physically secure location is subject to criminal justice agency management control. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled, and secured. Restricted non-public areas in the Thurston County Corrections Facility (TCCF) shall be identified with a sign at the entrance.

Visitors Access: Visitor specifications need to be established per agency purview and approval. A visitor is defined as a person who visits TCCF on a temporary basis who is not employed by the Thurston County Sheriff's Office and has no unescorted access to the physically secure location within the TCCF where FBI CJI and associated information systems are located.

TAC: Terminal Agency Coordinator. The point of contact within the agency who will serve as a liaison between the agency and the state ACCESS Auditors and Trainers.

LASO: Local Agency Security Officer

NCJA: Non-Criminal Justice Agency

210.4 PROCEDURES

Visitors must:

Copyright Lexipol, LLC 2025/01/02, All Rights Reserved.
Published with permission by Thurston County Sheriff's Office

(a) Check in before entering a physically secure location by:

  (a) Present acceptable identification as outlined in TCCF #41.A.05.

  (b) Wear approved visitor badge on approved visitor's outer clothing and returned to the agency at the end of the visit.

(b) Be accompanied by a TCCF escort at all times to include delivery or service personnel. An escort is defined as an authorized personnel who accompanies a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any CJI therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

(c) Show a valid form of photo identification.

(d) Follow TCCF procedures for authorized unescorted access.

  (a) Noncriminal Justice Agency (NCJA) such as IT who require frequent unescorted access to restricted area(s) will be required to establish a Management Control Agreement between the TCCF and NCJA. Each NCJA employee with CJI access will appropriately have state and national fingerprint-based record background check prior to this restricted area access being granted.

  (b) Private contractors/vendors who require frequent unescorted access to restricted area(s) will be required to establish a Security Addendum between the TCCF and each private contractor personnel. Each private contractor personnel will appropriately have state and national fingerprint-based record background check prior to this restricted area access being granted.

(e) Not be allowed to view screen information mitigating shoulder surfing.

(f) Individuals not having any legitimate business in a restricted area shall be courteously escorted to a public area of the facility. Strangers in physically secure areas without an escort should be challenged. If resistance or behavior of a threatening or suspicious nature is encountered, sworn personnel shall be notified or call 911.

(g) Not be allowed to sponsor another visitor.

(h) Not enter into a secure area with electronic devices unless approved by the TCCF Local Area Security Officer (LASO) to include cameras and mobile devices. Photographs are not allowed without permission of the TCCF assigned personnel.

(i) All requests by groups for tours of the TCCF facility will be referred to the proper agency point of contact for scheduling. In most cases, these groups will be handled by a single form, to be signed by a designated group leader or representative. Remaining visitor rules apply for each visitor within the group. The group leader will provide a list of names to front desk personnel for instances of emergency evacuation and accountability of each visitor while on agency premises.

210.5 AUTHORIZED PHYSICAL ACCESS

Only authorized personnel will have access to physically secure non-public locations. TCCF will maintain and keep current a list of authorized personnel. All physical access points into

Copyright Lexipol, LLC 2025/01/02, All Rights Reserved.
Published with permission by Thurston County Sheriff's Office

the agency's secure areas will be authorized before granting access.The agency will implement access controls and monitoring of physically secure areas for protecting all transmission and display mediums of CJI. Authorized personnel will take necessary steps to prevent and protect the agency from physical, logical and electronic breaches.

All personnel with CJI physical and logical access must:

(a) Meet the minimum personnel screening requirements prior to CJI access.

    (a) To verify identification, a state of residency and national fingerprint-based record checks shall be conducted prior to having unescorted access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.

    (b) Support personnel, private contractors/vendors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.

    (c) Prior to granting access to CJI, the TCCF on whose behalf the contractor is retained shall verify identification via a state of residency and national fingerprint-based record check.

    (d) Refer to the for handling cases of felony convictions, criminal records, arrest histories, etc.

(b) Complete security awareness training.

    (a) All authorized TCCF, Noncriminal Justice Agencies (NCJA) like city or county IT and private contractor/vendor personnel will receive security awareness training prior to being granted duties that require CJI access and annuallythereafter.

    (b) Security awareness training will cover areas specified in the at a minimum.

(c) Be aware of who is in their secure area before accessing confidential data.

    (a) Take appropriate action to protect all confidential data.

    (b) Protect all terminal monitors with viewable CJI displayed on monitor and not allow viewing by the public or escorted visitors.

(d) Properly protect and not share any individually issued keys, proximity cards, computer account passwords, etc.

    (a) Report loss of issued keys, proximity cards, etc to authorized agency personnel.

    (b) If the loss occurs after normal business hours, or on weekends or holidays, personnel are to call the TCCF POC to have authorized credentials like a proximity card de-activated and/or door locks possibly rekeyed.

    (c) Safeguard and not share passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and all other facility and computer systems security access procedures. See Disciplinary Policy.

(e) Properly protect from viruses, worms, Trojan horses, and other malicious code.

Copyright Lexipol, LLC 2025/01/02, All Rights Reserved.
Published with permission by Thurston County Sheriff's Office

(f) Web usage—allowed versus prohibited; monitoring of user activity.

(g) Do not use personally owned devices on the TCCF computers with CJI access. (Agency discretion). See Personally Owned Policy.

(h) Use of electronic media is allowed only by authorized TCCF personnel. Controls shall be in place to protect electronic media and printouts containing CJI while in transport. When CJI is physically moved from a secure location to a non-secure location, appropriate controls will prevent data compromise and/or unauthorized access.

(i) Encrypt emails when electronic mail is allowed to transmit CJI-related data as such in the case of Information Exchange Agreements.

  (a) If CJI is transmitted by email, the email must be encrypted and email recipient must be authorized to receive and view CJI.

(j) Report any physical security incidents to the TCCF's LASO to include facility access violations, loss of CJI, loss of laptops, Blackberries, thumb drives, CDs/DVDs and printouts containing CJI.

(k) Hard copy printouts of CJI will not be released to any agency (including law enforcement agencies). Most agencies that would request this information should have their own access or resource to obtain this information.

(l) Ensure data centers with CJI are physically and logically secure.

(m) Keep appropriate TCCF security personnel informed when CJI access is no longer needed. In the event of ended employment, the individual must surrender all property and access managed by the local agency, state and/or federal agencies.

(n) Not use food or drink around information technology equipment.

(o) Know which door to use for proper entry and exit of the TCCF and only use marked alarmed fire exits in emergency situations.

Ensure the perimeter security door securely locks after entry or departure. Do not leave any perimeter door propped opened and take measures to prevent piggybacking entries

210.6 ROLES AND RESPONSIBILITIES

Terminal Agency Coordinator (TAC)

The TAC serves as the point-of-contact at the TCCF for matters relating to CJIS information access. The TAC administers CJIS systems programs within the agency and oversees the agency's compliance with FBI and state CJIS systems policies.

Local Agency Security Officer (LASO)

Each LASO shall:

(a) Identify who is using the CSA (state) approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.

(b) Identify and document how the equipment is connected to the state system.

Copyright Lexipol, LLC 2025/01/02, All Rights Reserved.
Published with permission by Thurston County Sheriff's Office

(c) Ensure that personnel security screening procedures are being followed as stated in this policy.

(d) Ensure the approved and appropriate security measures are in place and working as expected.

(e) Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

Information Technology Support

In coordination with above roles, all vetted IT support staff will protect CJI from compromise at the TCCF by performing the following:

(a) Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed. Know where CJI is stored, printed, copied, transmitted and planned end of life. There is no authorization from TCCF to store CJI on laptops, mobile data terminals (MDTs), computers, servers, tape backups, CDs, DVDs, thumb drives, RISC devices and internet connections as authorized by the TCCF. For agencies who submit fingerprints using Live Scan terminals, only Live Scan terminals that receive CJI back to the Live Scan terminal will be assessed for physical security.

(b) Be knowledgeable of required TCCF technical requirements and policies taking appropriate preventative measures and corrective actions to protect CJI at rest, in transit and at the end of life.

(c) Take appropriate action to ensure maximum uptime of CJI and expedited backup restores by using agency approved best practices for power backup and data backup means such as generators, backup universal power supplies on CJI-based terminals, servers, switches, etc.

(d) Properly protect the TCCF's CJIS system(s) from viruses, worms, Trojan horses, and other malicious code (real-time scanning and ensure updated definitions).

    (a) Install and update antivirus on computers, servers, etc.

(e) Scan any outside non-agency owned CDs, DVDs, thumb drives, etc., for viruses, if the TCCF allows the use of personally owned devices.

(f) Data backup and storage—centralized or decentralized approach.

    (a) Perform data backups and take appropriate measures to protect all stored CJI.

    (b) Ensure only authorized vetted personnel transport off-site tape backups or any other media that store CJI that is removed from physically secured location.

    (c) Ensure any media released from the TCCF is properly sanitized / destroyed. (See Sanitization and Destruction Policy TCSO MASTER SOP section 20, pg. 65)

(g) Timely application of system patches—part of configuration management.

    (a) The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

Copyright Lexipol, LLC 2025/01/02, All Rights Reserved.
Published with permission by Thurston County Sheriff's Office

(b) When applicable, see the TCCF Patch Management Policy.

(h) Access control measures

(a) Address least privilege and separation of duties.

(b) Enable event logging of:

(a) Successful and unsuccessful system log-on attempts.

(b) Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.

(c) Successful and unsuccessful attempts to change account passwords.

(d) Successful and unsuccessful actions by privileged accounts.

(e) Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.

(c) Prevent authorized users from utilizing publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

(i) Account Management in coordination with TAC

1. Agencies shall ensure that all user IDs belong to currently authorized users.

2. Keep login access current, updated and monitored. Remove or disable terminated or transferred or associated accounts.

3. Authenticate verified users as uniquely identified.

4. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs.

5. Not use shared generic or default administrative user accounts or passwords for any device used with CJI.

6. Passwords

(a) Be a minimum length of eight (8) characters on all systems.

(b) Not be a dictionary word or proper name.

(c) Not be the same as the User ID.

(d) Expire within a maximum of 90 calendar days.

(e) Not be identical to the previous ten (10) passwords.

(f) Not be transmitted in the clear or plaintext outside the secure location.

(g) Not be displayed when entered.

(h) Ensure passwords are only reset for authorized user.

Copyright Lexipol, LLC 2025/01/02, All Rights Reserved.
Published with permission by Thurston County Sheriff's Office

(j) Network infrastructure protection measures.

(a) Take action to protect CJI-related data from unauthorized public access.

(b) Control access, monitor, enabling and updating configurations of boundary protection firewalls.

(c) Enable and update personal firewall on mobile devices if needed.

(d) Ensure confidential electronic data is only transmitted on secure network channels using encryption and *advanced authentication when leaving a physically secure location. No confidential data should be transmitted in clear text.

(e) No media will be removed from a physically secured location.

(f) Not use default accounts on network equipment that passes CJI like switches, routers, firewalls.

(g) Make sure law enforcement networks with CJI shall be on their own network accessible by authorized personnel who have been vetted by the TCCF. Utilize Virtual Local Area Network (VLAN) technology to segment CJI traffic from other noncriminal justice agency traffic to include other city and/or county agencies using same wide area network.

(k) Communicate and keep TCCF informed of all scheduled and unscheduled network and computer downtimes, all security incidents and misuse. The ultimate information technology management control belongs to Thurston County Central Services.

210.7 FRONT DESK AND VISITOR SPONSORING PERSONNEL

Administration of the Visitor Check-In / Check-Out procedure is the responsibility of identified individuals in each facility. This duty is done by the Reception Desk or Central Control.

Prior to visitor gaining access to physically secure area:

(a) The visitor will be screened by TCCF personnel for weapons. No weapons are allowed in the agency except when carried by authorized personnel as deemed authorized by TCCF.

(b) The visitor will be screened for electronic devices. No personal electronic devices are allowed in any agency facility except when carried by authorized personnel as deemed authorized by TCCF.

(c) Escort personnel will acknowledge being responsible for properly evacuating visitor in cases of emergency. Escort personnel will know appropriate evacuation routes and procedures.

(d) Escort and/or Front desk personnel will validate visitor is not leaving agency with any agency owned equipment or sensitive data prior to Visitor departure.

All TCCF personnel and supporting entities are responsible to report any unauthorized physical, logical, and electronic access to TCCF officials. For TCCF, the point of contacts to report any non-secure access is:

Copyright Lexipol, LLC 2025/01/02, All Rights Reserved.
Published with permission by Thurston County Sheriff's Office

LASO Name: B. Clark	LASO Phone:360-545-5196	LASO email:brett.clark@co.thurston.wa.us
AC Name: Jen McAneney	AC Phone: 360-709-5932	AC email:mcanenj@co.thurston.wa.us
State C/ISO Name:ACCESS	C/ISO Phone:360-534-2108	C/ISO email:access@wsp.wa.gov

Penalties:

Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and / or termination.

Violation of any of the requirements in this policy by any visitor can result in similar disciplinary action against the sponsoring employee, and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

Copyright Lexipol, LLC 2025/01/02, All Rights Reserved.
Published with permission by Thurston County Sheriff's Office